



Data Protection Policy

Contents

Purpose	1
Definitions	1
Data Protection Principles	3
Guidelines	5
Training	18
Links to other Policies and procedures	18
Approved	18
Document / Process Approval	19
Document / Process History	19
Document / Process Owner	19
Document / Process Review	19
Appendix 1: Subject Access Request Form (SAR)	20

Purpose

This policy applies to all of Green Light Trust’s activities where a Data Subject’s Personal Data is collected, processed, stored or destroyed. All trustees, employees, volunteers, contractors and anyone else who collects, processes, stores or destroys Personal Data on behalf of Green Light Trust should comply with this policy.

This policy is written to comply with the latest legislation for the protection of data, namely the Data Protection Act 2018 (and as it follows the EU GDPR legislation in force from 25th May 2018).

Definitions

Anonymisation: Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) by any means or by any person.

Consent: Explicit and freely given authorisation from the Data Subject that their Personal Data can be processed for the specific purposes clearly outlined to them.



Contact: Any past, current or prospective Green Light Trust customer, employee, volunteer, trustee, contractor, or anyone else from whom Personal Data is collected by Green Light Trust.

Data Controller: A natural or legal person, Public Authority, Agency, or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

Data Protection Officer (DPO): The person responsible for overseeing an organisation's Data Protection strategy and its implementation to ensure compliance with legal and regulatory requirements.

Encryption: The process of converting information or data into code, to prevent unauthorised access.

Identifiable Natural Person: Anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Personal Data: Any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person. For the purpose of clarification, this includes images of an Identifiable Natural Person.

Personal Data Breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed.

Profiling: Any form of automated processing of Personal Data where Personal Data is used to evaluate specific or general characteristics relating to an Identifiable Natural Person. In particular to analyse or predict certain aspects concerning that natural person's performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movement.

Pseudonymisation: Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) without a "key" that allows the data to be re-identified.

Special Categories of Data: The GDPR defines special category data as:

- personal data revealing **racial or ethnic origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious or philosophical beliefs**;



- personal data revealing **trade union membership**;
- **genetic data**;
- **biometric data** (where used for identification purposes);
- data concerning **health**;
- data concerning a person's **sex life**; and
- data concerning a person's **sexual orientation**.

Third Country: Any country not recognised as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Data.

Third Party: An organisation external to Green Light Trust (which includes any associated social enterprise organisations or persons that are considered part of Green Light Trust's network) with which Green Light Trust conducts business and is also authorised to, under the direct authority of Green Light Trust, process the Personal Data of Green Light Trust's Contacts

Policy Dissemination & Enforcement

The managers of each place where Green Light Trust activities relating to the collection, processing, storing or destruction of Personal Data is carried on, must ensure that all Green Light Trust persons responsible for Personal Data are aware of and comply with the contents of this policy.

In addition, each Green Light Trust manager will make sure all Third Parties engaged to processing Personal Data on their behalf (i.e. their Data Processors) are aware of and comply with the contents of this policy. Assurance of such compliance must be obtained from all Third Parties, whether companies or individuals, prior to granting them access to Personal Data controlled by Green Light Trust.

Data Protection by Design

To ensure that all Data Protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, each system or process must have due consideration of this policy and Green Light Trust's obligations under the relevant Data Protection legislation, before implementation.

Data Protection Principles

Green Light Trust has adopted the following principles to govern its collection, use, retention, transfer, disclosure and destruction of Personal Data:



Principle 1: Lawfulness, Fairness and Transparency

Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. This means, Green Light Trust must tell the Data Subject what processing will occur (transparency), the processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in the applicable Data Protection regulation (lawfulness).

Principle 2: Purpose Limitation

Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means Green Light Trust must specify exactly what the Personal Data collected will be used for and limit the processing of that Personal Data to only what is necessary to meet the specified purpose.

Principle 3: Data Minimisation

Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This means Green Light Trust must not store any Personal Data beyond what is strictly required.

Principle 4: Accuracy

Personal Data shall be accurate and kept up to date. This means Green Light Trust must have in place processes for identifying and addressing out-of-date, incorrect and redundant Personal Data.

Principle 5: Storage Limitation

Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is processed. This means Green Light Trust must, wherever possible, store Personal Data in a way that limits or prevents identification of the Data Subject.

Principle 6: Integrity & Confidentiality

Personal Data shall be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing, and against accidental loss, destruction or damage. Green Light Trust must use appropriate technical and organisational measures to ensure the integrity and confidentiality of Personal Data is maintained at all times.

Principle 7: Accountability



Each person responsible for Personal Data at Green Light Trust should be able to demonstrate compliance. This means they must demonstrate that the six Data Protection Principles (outlined above) are met for all Personal Data for which they are responsible.

Guidelines

3. Data Collection

3.3.1 Data Sources

Personal Data should be collected only from the Data Subject unless one of the following apply:

1. The nature of the business purpose necessitates collection of the Personal Data from other persons or bodies.
2. The collection must be carried out under emergency circumstances in order to protect the vital interests of the Data Subject or to prevent serious loss or injury to another person.

If Personal Data is collected from someone other than the Data Subject, the Data Subject must be informed of the collection unless one of the following apply:

1. The Data Subject has received the required information by other means
2. The information must remain confidential due to a professional secrecy obligation
3. Legislation expressly provides for the collection, processing or transfer of the Personal Data

Where it has been determined that notification to a Data Subject is required, notification should occur promptly, but in no case later than:

1. One calendar month from the first collection or recording of the Personal Data
2. At the time of first communication if used for communication with the Data Subject
3. At the time of disclosure if disclosed to another recipient.

3.3.2 Data Subject Consent

Each person acting on behalf of Green Light Trust will obtain Personal Data only by lawful and fair means and, where appropriate with the knowledge and Consent of the individual concerned.



Where a need exists to request and receive the Consent of an individual prior to the collection, use or disclosure of their Personal Data, Green Light Trust is committed to seeking such Consent.

Persons acting on behalf of Green Light Trust shall establish a system for obtaining and documenting Data Subject Consent for the collection, processing, and/or transfer of their Personal Data. The system must include provisions for:

1. Determining what disclosures should be made in order to obtain valid Consent.
2. Ensuring the request for Consent is presented in a manner which is clearly distinguishable from any other matters, is made in an intelligible and easily accessible form, and uses clear and plain language.
3. Ensuring the Consent is freely given (i.e. is not based on a contract that is conditional to the processing of Personal Data that is unnecessary for the performance of that contract).
4. Documenting the date, method and content of the disclosures made, as well as the validity, scope, and volition of the Consents given.
5. Providing a simple method for a Data Subject to withdraw their Consent at any time.

3.3.3 Data Subject Notification

Each person acting on behalf of Green Light Trust will, when required by applicable law, contract, or where they consider that it is reasonably appropriate to do so, provide Data Subjects with information as to the purpose of the processing of their Personal Data.

When the Data Subject is asked to give Consent to the processing of Personal Data and when any Personal Data is collected from the Data Subject, all appropriate disclosures will be made, in a manner that draws attention to them, unless one of the following apply:

1. The Data Subject already has the information
2. A legal exemption applies to the requirements for disclosure and/or Consent.

The disclosures may be given orally, electronically or in writing.

The associated receipt or form should be retained, along with a record of the facts, date, content, and method of disclosure.

3.3.4 External Privacy Notices



Each external website provided by Green Light Trust will include an online 'Privacy Notice' and an online 'Cookie Notice' fulfilling the requirements of applicable law.

3.4 Data Use

3.4.1 Data Processing

Green Light Trust uses the Personal Data of its Contacts for the following broad purposes:

1. The general running and business administration of Green Light Trust's processes.
2. To provide services to Green Light Trust customers
3. The ongoing administration and management of customer services
4. For employee, contractor, and volunteer management
5. For reporting programme outcomes to referrers or funders

The use of a Contact's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object. For example, it would clearly be within a Contact's expectations that their details will be used by Green Light Trust to respond to a Contact request for information about the services on offer. However, it will not be within their reasonable expectations that Green Light Trust would then provide their details to Third Parties for marketing purposes.

Each Green Light Trust representative will process Personal Data in accordance with all applicable laws and applicable contractual obligations. More specifically, Green Light Trust will not process Personal Data unless at least one of the following requirements are met:

1. The Data Subject has given Consent to the processing of their Personal Data for one or more specific purposes.
2. Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract
3. Processing is necessary for compliance with a legal obligation to which the Data Controller is subject
4. Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person.
5. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in Green Light Trust.



6. Processing is necessary for the purposes of the legitimate interests pursued by Green Light Trust or by a Third Party (except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject).

There are some circumstances in which Personal Data may be further processed for purposes that go beyond the original purpose for which the Personal Data was collected. When making a determination as to the compatibility of the new reason for processing, guidance and approval must be obtained from a Green Light Trust manager or trustee before any such processing may commence.

In any circumstance where Consent has not been gained for the specific processing in question, Green Light Trust will address the following additional conditions to determine the fairness and transparency of any processing beyond the original purpose for which the Personal Data was collected:

1. Any link between the purpose for which the Personal Data was collected and the reasons for intended further processing.
2. The context in which the Personal Data has been collected, in particular regarding the relationship between Data Subject and the Data Controller.
3. The nature of the Personal Data, in particular whether Special Categories of Data are being processed, or whether Personal Data related to criminal convictions and offences are being processed.
4. The possible consequences of the intended further processing for the Data Subject.
5. The existence of appropriate safeguards pertaining to further processing, which may include Encryption, Anonymisation or Pseudonymisation.

3.4.2 Special Categories of Data

Green Light Trust will only process Special Categories of Data (also known as sensitive data) where the Data Subject expressly consents to such processing or where one of the following conditions apply:

1. The processing relates to Personal Data which has already been made public by the Data Subject
2. The processing is necessary for the establishment, exercise or defence of legal claims
3. The processing is specifically authorised or required by law.
4. The processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent



5. Further conditions, including limitations, based upon legislation related to the processing of genetic data, biometric data or data concerning health

In any situation where Special Categories of Data are to be processed, prior approval must be obtained from a manager or trustee of Green Light Trust and the basis for the processing clearly recorded with the Personal Data in question.

Where Special Categories of Data are being processed, Green Light Trust will adopt adequate protection measures. Each Green Light Trust representative may also adopt additional measures to address local custom or social expectation over the processing of Special Categories of Data.

3.4.3 Criminal Offences and Convictions

Green Light Trust may process data relating to Criminal Offences and Convictions of its employees, trustees, volunteers, contractors or beneficiaries where the Data Subject expressly consents to such processing, and it is required or permissible to do so by law.

As Green Light Trust works with children and vulnerable adults and has a duty to safeguard them from risk, Disclosure and Barring (DBS) check processes are in place for all employees, trustees, volunteers and contractors.

Information regarding certain types of criminal offences and convictions may be collected directly from an individual or an authorised referring organisation representative and processed by Green Light Trust, where such individual will be receiving services from Green Light Trust and will be interacting with employees, volunteers, contractors, or children or vulnerable adults also receiving services from Green Light Trust.

For the purposes of processing this type of criminal offence or conviction data, Green Light Trust will apply the same conditions as in 3.4.2 above.

3.4.4 Data Quality

Each Green Light Trust representative will adopt all necessary measures to ensure that the Personal Data they collect and process is complete and accurate in the first instance, and is updated to reflect the current situation of the Data Subject.

The measures adopted by Green Light Trust to ensure data quality include:



1. Correcting Personal Data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the Data Subject does not request rectification
2. Keeping Personal Data only for the period necessary to satisfy the permitted uses or applicable statutory retention period
3. The removal of Personal Data if in violation of any of the Data Protection principles or if the Personal Data is no longer required
4. Restriction, rather than deletion of Personal Data, insofar as:
 - a. A law prohibits erasure
 - b. Erasure would impair legitimate interests of the Data Subject
 - c. The Data Subject disputes that their Personal Data is correct and it cannot be clearly ascertained whether their information is correct or incorrect

3.4.5 Profiling & Automated Decision-Making

Green Light Trust will only engage in Profiling and automated decision-making where it is necessary to enter into, or to perform, a contract with the Data Subject or where it is authorised by law.

Where a Green Light Trust representative utilises Profiling and automated decision-making, this will be disclosed to the relevant Data Subjects. In such cases the Data Subjects will be given the opportunity to:

1. Express their point of view
2. Obtain an explanation for the automated decision
3. Review the logic used by the automated system
4. Supplement the automated system with additional data
5. Have a human carry out a review of the automated decision
6. Contest the automated decision
7. Object to the automated decision-making being carried out

Each Green Light Trust representative must also ensure that all Profiling and automated decision-making relating to a Data Subject is based on accurate data.

3.4.6 Digital Marketing

As a general rule Green Light Trust will not send promotional or direct marketing material to a Green Light Trust Contact through digital channels such as mobile phones, email and the Internet, without first obtaining their Consent. Any Green Light Trust representative wishing to carry out a digital marketing campaign without obtaining prior Consent from the Data Subject must first have it approved by a senior manager.



Where Personal Data processing is approved for digital marketing purposes, the Data Subject must be informed at the point of first contact that they have the right to object, at any stage, to having their data processed for such purposes. If the Data Subject puts forward an objection, digital marketing related processing of their Personal Data must cease immediately and their details should be kept on a suppression list with a record of their opt-out decision, rather than being completely deleted.

It should be noted that where digital marketing is carried out in a 'business to business' context, there is no legal requirement to obtain an indication of Consent to carry out digital marketing to individuals provided that they are given the opportunity to opt-out.

3.5 Data Retention

To ensure fair processing, Personal Data will not be retained by Green Light Trust for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed.

The length of time for which Green Light Trust retains Personal Data is set out below:

	Suppliers/ contractors	Employees/Volunteers	Participants /clients
Finance data and systems	7 years	7 Years	7 Years
Case Management Systems	3 years	3 years (unless otherwise stated for funding purposes)	3 years (unless otherwise stated for funding purposes)
HR systems	6 years	6 years (following departure from GLT)	N/A

This takes into account any legal and contractual requirements, both minimum and maximum, that influence the retention periods. All Personal Data should be securely deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

3.6 Data Protection

Each Green Light Trust representative will adopt physical, technical, and organisational measures to ensure the security of Personal Data. This



includes the prevention of loss or damage, unauthorised alteration, access or processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment.

A summary of the Personal Data related security measures is provided below:

1. Prevent unauthorised persons from gaining access to data processing systems in which Personal Data are processed
2. Prevent persons entitled to use a data processing system from accessing Personal Data beyond their needs and authorisations.
3. Ensure that all Personal Data are stored on electronic devices that can only be accessed by authorised personnel, that are password protected and that firewall protection is in place and kept up to date.
4. Ensure that Personal Data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorisation
5. Ensure that access logs are in place to establish whether, and by whom, the Personal Data was entered into, modified on or removed from a data processing system
6. Ensure that in the case where processing is carried out by a Data Processor, the data can be processed only in accordance with the instructions of the Data Controller
7. Ensure that Personal Data is protected against undesired destruction or loss
8. Ensure that Personal Data collected for different purposes can and is processed separately
9. Ensure that Personal Data is not kept longer than necessary
10. Ensure that express permission is obtained from a Data Subject prior to publication of images or any other Personal Data on any form of public or social media
11. Ensure that any hard copies of Personal Data being disposed of are shredded and disposed of as confidential waste.

3.7 Data Subject Requests

The Business and Systems Manager/Deputy DPO will establish a system to enable and facilitate the exercise of Data Subject rights related to:

1. Information access
2. Objection to processing
3. Objection to automated decision-making and Profiling
4. Restriction of processing
5. Data portability
6. Data rectification
7. Data erasure



If an individual makes a request relating to any of the rights listed above, Green Light Trust will consider each such request in accordance with all applicable Data Protection laws and regulations.

No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature.

Data Subjects are entitled to obtain, based upon a request made in writing to Green Light Trust and upon successful verification of their identity, the following information about their own Personal Data:

1. The purposes of the collection, processing, use and storage of their Personal Data
2. The source(s) of the Personal Data, if it was not obtained from the Data Subject
3. The categories of Personal Data stored for the Data Subject
4. The recipients or categories of recipients to whom the Personal Data has been or may be transmitted, along with the location of those recipients
5. The envisaged period of storage for the Personal Data or the rationale for determining the storage period
6. The use of any automated decision-making, including Profiling
7. The right of the Data subject to:
 - a. Object to processing of their Personal Data
 - b. Lodge a complaint with the Information Commissioner's Office
 - c. Request rectification or erasure of their Personal Data
 - d. Request restriction of processing of their Personal Data

All requests for access to Personal Data should be referred to Green Light Trust's Business and Systems Manager, who should log each request as it is received. A response to each request will be provided within 30 days of the receipt of the written request from the Data Subject. Appropriate verification must confirm that the requestor is the Data Subject or their authorised legal representative. Data Subjects shall have the right to require Green Light Trust to correct or supplement erroneous, misleading, outdated, or incomplete Personal Data.

If Green Light Trust cannot respond fully to the request within 30 days, the Business and Systems Manager shall nevertheless provide the following information to the Data Subject, or their authorised legal representative within the specified time:

1. An acknowledgement of receipt of the request
2. Any information located to date



3. Details of any requested information or modifications which will not be provided to the Data Subject, the reason(s) for the refusal, and any procedures available for appealing the decision
4. An estimated date by which any remaining responses will be provided
5. An estimate of any costs to be paid by the Data Subject (e.g. where the request is excessive in nature)
6. The name and contact information of Green Light Trust individual who the Data Subject should contact for follow up

It should be noted that situations may arise where providing the information requested by a Data Subject would disclose Personal Data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights.

Please refer to Subject Access Request form in the appendix

3.8 Law Enforcement Requests & Disclosures

In certain circumstances, it is permitted that Personal Data be shared without the knowledge or Consent of a Data Subject. This is the case where the disclosure of the Personal Data is necessary for any of the following purposes:

1. The prevention or detection of crime
2. The apprehension or prosecution of offenders
3. The assessment or collection of a tax or duty
4. By the order of a court or by any rule of law

If a Green Light Trust representative processes Personal Data for one of these purposes, then they may apply an exception to the processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice the case in question.

If any Green Light Trust representative receives a request from a court or any regulatory or law enforcement authority for information relating to a Green Light Trust Contact, they must immediately notify the Administration Manager who will provide comprehensive guidance and assistance.

3.9 Data Protection Training

All Green Light Trust employees, trustees, volunteers, contractors or any other representatives of Green Light Trust that have access to Personal Data will have their responsibilities under this policy outlined to them as part of their training or contractual obligations. In addition, each Green Light Trust location manager will provide any necessary ongoing Data



Protection training and procedural guidance for their employees or any other relevant persons.

The training and procedural guidance set forth will consist of, at a minimum, the following elements:

1. The Data Protection Principles set forth in Section **3.2** above
2. Each person's duty to use and permit the use of Personal Data only by authorised persons and for authorised purposes
3. The need for, and proper use of, the forms and procedures adopted to implement this policy
4. The correct use of passwords, security tokens and other access mechanisms
5. The importance of limiting access to Personal Data, such as by using password protected screen savers and logging out when systems are not being attended by an authorised person
6. Securely storing manual files, print outs and electronic storage media
7. The need to obtain appropriate authorisation and utilise appropriate safeguards for all transfers of Personal Data outside of the internal network and physical office premises
8. Proper disposal of Personal Data by using secure shredding facilities
9. Any special risks associated with particular departmental activities or duties

3.10 Data Transfers

Green Light Trust representatives may transfer Personal Data to internal or Third Party recipients located in another country where they are authorised by a Green Light Trust manager or trustee to do so and where that country is recognised as having an adequate level of legal protection for the rights and freedoms of the relevant Data Subjects.

Where transfers need to be made to countries lacking an adequate level of legal protection (i.e. Third Countries), they must be made in compliance with an approved transfer mechanism.

Green Light Trust representatives may only transfer Personal Data where one of the transfer scenarios listed below applies:

1. The Data Subject has given Consent to the proposed transfer
2. The transfer is necessary for the performance of a contract with the Data Subject
3. The transfer is necessary for the implementation of pre-contractual measures taken in response to the Data Subject's request



4. The transfer is necessary for the conclusion or performance of a contract concluded with a Third Party in the interest of the Data Subject
5. The transfer is legally required on important public interest grounds
6. The transfer is necessary for the establishment, exercise or defence of legal claims
7. The transfer is necessary in order to protect the vital interests of the Data Subject

3.10.1 Transfers between Green Light Trust persons or locations

In order for Green Light Trust to carry out its operations effectively across its various locations or departments, there may be occasions when it is necessary to transfer Personal Data from one Green Light Trust person, department or location to another, or to allow access to the Personal Data from an overseas location. Should this occur, the Green Light Trust representative sending the Personal Data remains responsible for ensuring protection for that Personal Data and should comply with the terms of this policy.

If transferring Personal Data electronically, it is either password protected or is sent using a secure transfer system such as Egress.

3.10.2 Transfers to Third Parties

Each Green Light Trust representative will only transfer Personal Data to, or allow access by, Third Parties when it is assured that the information will be processed legitimately and protected appropriately by the recipient. Where Third Party processing takes place, each Green Light Trust representative will first identify if, under applicable law, the Third Party is considered a Data Controller or a Data Processor of the Personal Data being transferred.

Where the Third Party is deemed to be a Data Controller, Green Light Trust will enter into an appropriate agreement with the Controller to clarify each party's responsibilities in respect to the Personal Data transferred.

Where the Third Party is deemed to be a Data Processor, Green Light Trust will enter into an adequate processing agreement with the Data Processor. The agreement must require the Data Processor to protect the Personal Data from further disclosure and to only process Personal Data in compliance with Green Light Trust's instructions. In addition, the agreement will require the Data Processor to implement appropriate technical and organisational measures to protect the Personal Data as well as procedures for providing notification of Personal Data Breaches.



When Green Light Trust is outsourcing services to a Third Party (including Cloud Computing services), it will identify whether the Third Party will process Personal Data on its behalf and whether the outsourcing will entail any Third Country transfers of Personal Data. In either case, it will make sure to include adequate provisions in the outsourcing agreement for such processing and Third Country transfers.

If transferring Personal Data electronically, it is either password protected or is sent using a secure transfer system such as Egress.

3.10 Complaints Handling

Data Subjects with a complaint about the processing of their Personal Data, should put forward the matter in writing to Green Light Trust. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. Green Light Trust will inform the Data Subject of the progress and the outcome of the complaint within a reasonable period.

If the issue cannot be resolved through consultation between the Data Subject and Green Light Trust, then the Data Subject may, at their option, seek redress through mediation, binding arbitration, litigation, or via complaint to the Information Commissioner's Office (UK) or Data Protection Authority within the applicable jurisdiction.

3.12 Breach Reporting

Any individual who suspects that a breach of security of data has occurred due to the loss, theft or exposure of Personal Data should immediately notify Green Light Trust's Business and Systems Manager, who should immediately notify Green Light Trust's Data Protection Officer (DPO), providing a description of what occurred.

Any suspected breach of security of Data, will be recorded and assessed to determine which Manager will investigate all reported incidents to confirm whether or not a breach of security of Personal Data has occurred. If a Personal Data breach is confirmed, the Business and Systems Manager will follow the relevant procedure based on the criticality and quantity of the Personal Data involved. Relevant data subjects will be contacted by Green Light Trust to advise that their Personal Data may have been lost, stolen or exposed and what action Green Light Trust are taking to address the issue. For severe Personal Data Breaches, Green Light Trust's Board of Trustees will initiate and chair an emergency response team to coordinate and manage the Personal Data breach. Where required by legislation, the Deputy DPO and/or DPO will report the breach to the Information Commissioner's Office (ICO). Green Light Trust is registered with the ICO under reference number: ZA308907.



4. Policy Maintenance

All inquiries about this policy, including requests for exceptions or changes should be directed in the first instance to the Green Light Trust Business and Systems Manager.

4.1 Publication

This policy shall be available to all Green Light Trust employees and relevant volunteers, contractors and other representatives of Green Light Trust.

Green Light Trust employees, trustees, volunteers and contractors should follow Green Light Trust's Code of Practice for Data Protection, which gives guidance on the application of this policy to everyday working practices.

4.2 Responsibilities

Green Light Trust's DPO is Lauren Shand (CEO). The Business and Systems Manager, Deputy DPO, is responsible overall for this Policy and its implementation. Notice of significant revisions shall be provided to Green Light Trust employees and relevant volunteers, contractors and other representatives by the Business and Systems Manager.

Training

Mandatory reading of policy on Breathe HR GDPR training.

Links to other Policies and procedures

Subject Access Request Form (see Appendix 1)
Data Protection Code of Practice
Privacy and Cookies Policy

Approved

Name

Lauren Shand

Signature



Position	Chief Executive
-----------------	------------------------

Date	13/08/2024
-------------	-------------------

Document / Process Approval

Version	Date	Approved By	Position
0.1	12/03/2023	Lauren Shand	Operations Director
1	07/12/2023	Lauren Shand	Chief Executive
2	13/08/2024	Lauren Shand	Chief Executive

Document / Process History

Author	Status	Version	Date	Description
Mandy Horne	Updated for review and issued	0.1	12/03/2023	Replacing version
Mandy Horne / Tina Brown	Updated for review and issued	1	07/12/2023	Review and amendments whole document
Tina Brown	Updated for review	2	01/08/2024	Updated document referencing Administration Manager, replaced throughout with Business and Systems Manager / and/or Deputy DPO & DPO

Document / Process Owner

Name	Position
Tina Brown	Business and Systems Manager

Document / Process Review

Document to be reviewed yearly or sooner if significant changes occur



Appendix 1: Subject Access Request Form (SAR)

Ask for copies of your data:

You have the right to ask for copies of your personal data we store and use. This is your right of access, also known as making a subject access request or SAR. We'll normally respond at the latest within one calendar month of receiving your request. There may be times where we need longer or we may need to charge a reasonable fee for admin costs. We'll let you know if this is the case.

You don't have to use this form to ask for copies of your data, but it's helpful for us to know what you're looking for so we can respond fully and promptly.

Please send your completed form to us using the contact details at the bottom of the page.

You can read more about your right of access by visiting:

<https://ico.org.uk/for-the-public/your-right-to-get-copies-of-your-data/>

Who's making this request?

We're asking for your contact details so we can send your response and discuss your request with you (if needed). You only need to give us relevant details. For example, you only need to give us your postal address if you'd like us to respond by post or if you think it would help us identify you. We may ask you for proof of ID if we feel it's reasonable and proportionate. The timescale for responding to your request will start when we receive this.

Your name

Contact number

Email address

Postal address

Are you making this request on behalf of someone else?

Yes

No (Please move to section three)

Please provide contact details of the person you are making the request for.

Name of other person

Contact number

Email address

Postal address



Other contact information for the person you are making the request for:

You also need to give us proof of your authority to act on their behalf. For example, this could be written authorisation from them or a relevant power of attorney.

Please send proof of authority together with this form when you make your request.

- Yes, I've got proof of my authority to act on someone else's behalf and I'll include it with my form. (Please move to section four.)
- No, I haven't got any proof of authority yet, but will send it at a later date. I understand you can't action my request until you receive this information.

How would you like us to respond to you?

We'll try and respond to you in the way that suits you. Please let us know if you need us to make any adjustments for you e.g. large font.

- Email**
- Post**
- Other (please specify)**

What personal data are you requesting?

If you know exactly what personal data you're looking for, it's helpful if you let us know.

For example, if you need a specific email, we could search for this using a particular word or phrase.

Briefly describe your request:

Is there a date range of the personal data you're asking for?

It's helpful if you're as specific as possible about your request. For example, if you've been a customer for several years, but you only need data about your recent purchase history, you could ask for data about things you've bought only in the last few months.

Date from

Date to

Can you tell us anything else to help us with our search?



If there's anything else of relevance you can tell us to help us identify you or the data you're requesting, please include this here. For example, any aliases, date of birth, order number or a customer reference number.

Further information to help us find the data you need

Thank you. We'll be in touch. If you'd like more information about how we use your data, have a look at our [\[add a link to your privacy notice\]](#).